Integrate Fortinet Firewall
EventTracker v8.x and above
Abstract

This guide provides instructions to configure Fortinet Firewall to send crucial events to EventTracker Enterprise by means of syslog.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 8.X and later, and Fortinet Firewall with FortiOS version 4.0-6.0.

Audience

Fortinet Firewall users, who wish to forward its events to EventTracker Manager and monitor them using EventTracker Enterprise.
# Table of Contents

Abstract ................................................................................................................................................................. 1  
Scope .................................................................................................................................................................. 1  
Audience .............................................................................................................................................................. 1  
Overview ............................................................................................................................................................. 3  
Prerequisites .......................................................................................................................................................... 3  
Enable Syslog Forwarding in FortiOS V4.0 ............................................................................................................ 3  
Enable Syslog Forwarding in FortiOS v5.0-6.0 ......................................................................................................... 4  
EventTracker Knowledge Pack .................................................................................................................................. 5  
Alerts ....................................................................................................................................................................... 5  
Flex Reports .......................................................................................................................................................... 5  
Import Fortinet Firewall Knowledge Pack into EventTracker .................................................................................. 12  
Import Alerts ....................................................................................................................................................... 13  
Import Knowledge Object ....................................................................................................................................... 14  
Token Template .................................................................................................................................................... 16  
Import Flex Reports ............................................................................................................................................ 17  
Verify Fortinet Firewall Knowledge Pack .............................................................................................................. 19  
Verify Alerts ........................................................................................................................................................ 19  
Verify Knowledge Object ...................................................................................................................................... 20  
Token Template .................................................................................................................................................... 20  
Verify Flex Reports ............................................................................................................................................. 21  
Create Dashboards in EventTracker ...................................................................................................................... 22  
Schedule Reports .................................................................................................................................................. 22  
Create Dashlets ................................................................................................................................................... 24  
Sample Dashboards ............................................................................................................................................. 28
Overview

Fortinet Firewall is one of the fastest firewall providing protection in various areas with other key security features such as anti-virus, intrusion prevention system (IPS), web filtering, anti-spam and traffic shaping to deliver multi-layered security for the IT environment.

EventTracker collects and analyses firewall events and enlightens an administrator about security violations, user behavior, and traffic anomalies.

Prerequisites

- EventTracker should be installed.
- Fortinet Firewall with FortiOS V4.0-V6.0 should be installed.

Enable Syslog Forwarding in FortiOS V4.0

Syslog is a standard for forwarding log messages in an IP network. Syslog captures log information provided by network devices.

1. To send logs to syslog server, click Log&Report, click Log Config, and then click Log Setting.
2. In the Logging and Archiving section, select Syslog option.

Figure 1
After you select the check box, the **Syslog** options appear.

3. Enter the appropriate information for the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP/FDQN</td>
<td>Enter the domain name or IP address of the syslog server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter port number for communication with the syslog server, usually port 514.</td>
</tr>
<tr>
<td>Minimum log level</td>
<td>Select a log level the Fortinet unit will log all messages at and above that logging severity level.</td>
</tr>
<tr>
<td>Facility</td>
<td>Facility indicates to the syslog server the source of a log message. By default, the Fortinet reports facility as local7. You can change the Facility if you want to distinguish log messages from different Fortinet units.</td>
</tr>
<tr>
<td>Enable CSV Format</td>
<td>Select to have logs formatted in CSV format. When you enable CSV format, the Fortinet unit produces the log in Comma Separated Value (CSV) format. If you do not enable CSV format, the Fortinet unit produces plain text files.</td>
</tr>
</tbody>
</table>

4. Select the **Apply** button.

**Enable Syslog Forwarding in FortiOS v5.0-6.0**

Use this command to configure log settings for logging to a remote syslog server (available only in the CLI)

You can configure the Fortinet unit to send logs to a remote computer running a syslog server.

Using the CLI, you can send logs to up to three different syslog servers. Configure additional syslog servers using syslogd2 and syslogd3 commands.

**Syntax:**

```
Config log {syslogd | syslogd2 | syslogd3} setting
```

- Enter `enable` to enable logging to a remote syslog server. Example: `set status enable`
- Enter `enable` to enable the Fortinet unit to produce the log in Comma Separated Value (CSV) format. If you do not enable CSV format the Fortinet unit produces plain text files.
Example: **set csv enable**

- Enter the facility type. Facility identifies the source of the log message to syslog.
  
  ```
  Example: set facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp | kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail | news | ntp | syslog | user | uucp}
  ```
  
  Example: **set facility local3**

- Enter the port number for communication with the syslog server.
  Example: **set port 514**

- Enable reliable delivery of syslog messages to the syslog server.
  Example: **set reliable enable**

- Enter the IP address of the syslog server that stores the logs.
  Example: **set server 172.168.22.54**

- Enter source IP address for syslogd, syslog2 and syslog3.
  Example: **set source-ip 172.168.22.50**

---

**EventTracker Knowledge Pack**

Once logs are received into EventTracker, Categories and reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Windows.

**Alerts**

- **Fortinet: Administrator logon failed**: This alert is generated when an administrator does a login failure.
- **Fortinet: Attack detected**: This alert is generated when any IPS alert is detected by Fortinet firewall.
- **Fortinet: Configuration changes**: This alert is generated when any configuration change is done in the Fortinet firewall.
- **Fortinet: Virus detected**: This alert is generated when any virus is detected by the Fortinet firewall.
- **Fortinet: Data leak protection**: This alert is generated when any DLP event is occurred.

**Flex Reports**

- **Fortinet- User authentication details**: This report provides details about all the user authentication details.
Integrate Fortinet Firewall

Logs Considered:

- **Fortinet- Administrator logon details**- This report provides details about all the admin login and logout activities.

![Log Time Table Example](image)

![Log Time Table Example](image)

![Log Time Table Example](image)
Logs Considered:

- **Fortinet- Attack detected** - This report provides details about all the IPS and IDS attacks that are detected by the Fortinet firewall.

- **Fortinet- Suspicious web content detected** - This report provides details about all the suspicious web traffic content that is detected by the Fortinet firewall.
### Logs Considered:

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Event ID</th>
<th>Site / Computer</th>
<th>User</th>
<th>Domain</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013-10-30 11:45:00</td>
<td>Fortinet- Suspicious email content detected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013-10-30 11:45:00</td>
<td>Fortinet- Data leak detected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Fortinet- Suspicious email content detected
- This report provides details about all the suspicious email traffic content that is detected by the Fortinet firewall.

#### Fortinet- Data leak detected
- This report provides details about all the DLP event that is detected by the Fortinet firewall.
Integrate Fortinet Firewall

Logs Considered:

- **Fortinet- Virus detected**- This report provides details about all the virus that is detected by the Fortinet firewall.

- **Fortinet- Traffic allowed details**- This report provides details about all the traffic that is allowed by the Fortinet firewall.

- **Fortinet- Traffic denied details**- This report provides details about all the traffic that is denied by the Fortinet firewall.
Integrate Fortinet Firewall

Logs Considered:

• **Fortinet- VPN logon details** - This report provides details about all the VPN logon details.

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Event ID</th>
<th>Site / Computer</th>
<th>User</th>
<th>Domain</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/30/2017 04:55:51 PM</td>
<td>2333</td>
<td>FORTINET</td>
<td>NA</td>
<td>NA</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FG3000C38136</td>
<td>06597</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>User Name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source IP Address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source Port</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Destination Port</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Action</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Logs Considered:

• **Fortinet- Configuration changes** - This report provides details about all the configuration changes that is done in the Fortinet firewall.

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Event ID</th>
<th>Site / Computer</th>
<th>User</th>
<th>Domain</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/30/2017 04:55:51 PM</td>
<td>2333</td>
<td>FORTINET</td>
<td>NA</td>
<td>NA</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FG3000C38136</td>
<td>06597</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>User Name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source IP Address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source Port</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Destination Port</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Action</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Logs Considered:

- **Fortinet- Application control** - This report provides details about all the application control policies and rules that is defined by the Fortinet firewall.
Integrate Fortinet Firewall

Logs Considered:

<table>
<thead>
<tr>
<th>LOG TIME</th>
<th>EVENT ID</th>
<th>SITE / COMPUTER</th>
<th>USER</th>
<th>DOMAIN</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/30/2017 5:21:39 PM</td>
<td>6333</td>
<td>NTPLDTRI59 / Fortin...</td>
<td>N/A</td>
<td>N/A</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

Example Event:
- **Event Type:** Information
- **Log Type:** Application
- **Category:** ID: 0
- **Description:**
  - Step 06: 18:24:29
  - date:2017-09-26
  - time:18:24:29
  - devname:4RT123
  - devid:050013815605932
  - logtype:10996028704
  - type: "sql" subtype="app-ctr
  - f" eventtype="app-ctrl.alt" level="information" vcls="log" logtime="1504722269" appid="159232 srcid="192.168.11.101 dstid="172.16.0.41.111 sqltype="448 srvtype="port12 strvalue="http" dstrvalue="wan" proto=6 service="HTTPS" policyid="253 sessionid="177512625 appid="p
  - elmer:Application Control Internet" appid="SocialMedia" appid="facebook" action=4 host="facebook.com" incidencenr="443334106 url=http://facebook.com" appid="medium" srcname="facebook.com"

### Import Fortinet Firewall Knowledge Pack into EventTracker

**NOTE:** Import knowledge pack items in the following sequence:

- Knowledge Objects
- Alerts
- Token Templates
- Flex Reports

**NOTE:** Export knowledge pack items in the following sequence:

- Knowledge Objects
- Alerts
- Token Templates
- Flex Reports

1. **Launch EventTracker Control Panel.**

2. Double click **Export Import Utility**, and then click the **Import** tab.
Import Alerts

1. Click **Alert** option, and then click the **browse** button.
2. Locate **Fortinet Firewall.isalt** file, and then click the **Open** button.

3. To import alerts, click the **Import** button.

4. EventTracker displays success message.

![Figure 3](image)

5. Click the **OK** button, and then click the **Close** button.

**Import Knowledge Object**

1. Click the **Admin** menu, and then click **Knowledge Objects**.

2. Click on the **Import** option.

![Figure 4](image)
3. In **IMPORT** pane click on **Browse** button.

![IMPORT](image1)

Figure 5

4. Locate **Fortinet.etko** file, and then click the **UPLOAD** button.

![IMPORT](image2)

Figure 6

5. Now select the check box and then click on ‘**OVERWRITE**’ option. EventTracker displays success message.
6. Click on OK button.

**Token Template**

1. Click the Admin menu, and then click Parsing rule.

2. Select Template tab, and then click on ‘Import’ option.

3. Click on Browse button.

4. Locate Fortinet Firewall Latest.ettd file, and then click the Open button.
5. Now select the check box and then click on ‘Import’ option. EventTracker displays success message.

![Figure 10](image1.png)

6. Click on OK button.

**Import Flex Reports**

1. Click Reports option, and then click the ‘browse’ button.
2. Locate applicable Fortinet Firewall.issch file, and then click the Open button.

![Figure 11](image2.png)
3. To import scheduled reports, click the **Import** button.

![Figure 12](image12.png)

4. EventTracker displays success message.

![Figure 13](image13.png)

5. Click **OK**, and then click the **Close** button.
Verify Fortinet Firewall Knowledge Pack

Verify Alerts

1. Logon to EventTracker Enterprise.

2. Click the Admin menu, and then click Alerts.

3. In the Search box, type ‘Fortinet’, and then click the Go button.

Alert Management page will display all the imported alerts.

4. To activate the imported alerts, select the respective checkbox in the Active column.

EventTracker displays message box.

5. Click OK, and then click the Activate Now button.
NOTE: Please specify appropriate systems in alert configuration for better performance.

Verify Knowledge Object

1. Click the Admin menu, and then click Knowledge Objects
2. Scroll down and select Fortinet in Objects pane.
   Imported Fortinet object details are shown.

![Knowledge Object](Image)

Figure 16

Token Template

1. Logon to EventTracker Enterprise web interface.
2. Click the Admin menu, and then click Parsing Rules and click Template.
3. Click on Fortinet Firewall group option.
Verify Flex Reports

1. Logon to EventTracker Enterprise.
2. Click the Reports menu, and then Configuration.
4. In Report Groups Tree to view imported Scheduled Reports, scroll down and click Fortinet Firewall group folder.

Scheduled Reports are displayed in the Reports configuration pane.
NOTE: Please specify appropriate systems in report wizard for better performance.

Create Dashboards in EventTracker

Schedule Reports

1. Open EventTracker in browser and logon.

2. Navigate to Reports>Configuration.
3. Select **Fortinet Firewall** in report groups. Check **defined** dialog box.

4. Click on ‘**schedule**’ to plan a report for later execution.
5. Choose appropriate time for report execution and in Step 8 check **Persist data in Eventvault explorer** box.

![Figure 22](image)

6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.

7. Proceed to next step and click **Schedule** button.

8. Wait for scheduled time or generate report manually.

**Create Dashlets**

1. **EventTracker 8** is required to configure flex dashboard.

2. Open **EventTracker** in browser and logon.
3. Navigate to **Dashboard>Flex**. Flex Dashboard pane is shown.

4. Click + to add a new dashboard. Flex Dashboard configuration pane is shown.
5. Fill fitting title and description and click **Save** button.

6. Click ✉️ to configure a new flex dashlet. Widget configuration pane is shown.

7. Locate earlier scheduled report in **Data Source** dropdown.
8. Select **Chart Type** from dropdown.
9. Select extent of data to be displayed in **Duration** dropdown.
10. Select computation type in **Value Field Setting** dropdown.
11. Select evaluation duration in **As Of** dropdown.
12. Select comparable values in **X Axis** with suitable label.
13. Select numeric values in **Y Axis** with suitable label.
14. Select comparable sequence in **Legend**.
15. Click **Test** button to evaluate. Evaluated chart is shown.
16. If satisfied, Click **Configure** button.

17. Click ‘customize’ 📈 to locate and choose created dashlet.

18. Click + to add dashlet to earlier created dashboard.
Sample Dashboards

- **REPORT:** Fortinet-Administrator logon details
  - **WIDGET TITLE:** Fortinet-Administrator logon details
  - **CHART TYPE:** Stacked Column
  - **AXIS LABELS [X-AXIS]:** User Name
  - **LEGEND [SERIES]:** Action
- REPORT: Fortinet-Application control
  WIDGET TITLE: Fortinet-Application control
  CHART TYPE: Pie
  AXIS LABELS [X-AXIS]: Application Name
  LEGEND [SERIES]: Action

![Pie Chart Image]

Action: “pass”

Legend:
- Microsoft.SharePoint
- Microsoft.Portal
- HTTPS.BROWSER
- Facebook
- BBC

10/29 17:21 - 10/30 17:21
• REPORT: Fortinet-Attack detected
  WIDGET TITLE: Fortinet-Attack detected
  CHART TYPE: Stacked Column
  AXIS LABELS [X-AXIS]: Attack Name
  LEGEND [SERIES]: Action
• REPORT: Fortinet-Data Leak Detected
  WIDGET TITLE: Fortinet-Data Leak Detected
  CHART TYPE: Stacked Column
  AXIS LABELS [X-AXIS]: Threat Name
  LEGEND [SERIES]: Severity

![Stacked Column Chart](image-url)
• REPORT: Fortinet-Suspicious Email Content Detected
  WIDGET TITLE: Fortinet-Suspicious Email Content Detected
  CHART TYPE: Stacked Column
  AXIS LABELS [X-AXIS]: Sender Address
  LEGEND [SERIES]: Attachment
• REPORT: Fortinet-Traffic denied details
  WIDGET TITLE: Fortinet-Traffic denied details
  CHART TYPE: Donut
  AXIS LABELS [X-AXIS]: Source IP Address
  LEGEND [SERIES]: Action

![FORTINET-TRAFFIC DENIED DETAILS Chart]

Action: deny

- 192.168.11.101
- 116.29.117.125
- 100.166.82.181

10/29 17:21 - 10/30 17:21
• **REPORT: Fortinet-User authentication details**
  - **WIDGET TITLE:** Fortinet-User authentication details
  - **CHART TYPE:** Stacked Column
  - **AXIS LABELS [X-AXIS]:** User Name
  - **LEGEND [SERIES]:** Action

![Fortinet-User Authentication Details Chart](image)
- **REPORT**: Fortinet-Virus detected
  - **WIDGET TITLE**: Fortinet-Virus detected
  - **CHART TYPE**: Stacked Column
  - **AXIS LABELS [X-AXIS]**: Virus Name
  - **LEGEND [SERIES]**: Reference Url

![Fortinet-Virus Detected Chart]

- Series: Reference Url
- 0-6 range on the Y-axis
- Virus names on the X-axis:
  - "Elcar" (4 units)
  - "Zap" (2 units)

Legend:
- Green: http://www.fortinet.com/be?vid=64
- Gray: http://www.fortinet.com/ve?vid=0

10/29 17:21 - 10/30 17:21
• REPORT: Fortinet-VPN logon details
  WIDGET TITLE: Fortinet-VPN logon details
  CHART TYPE: Stacked Column
  AXIS LABELS [X-AXIS]: Source IP Address
  LEGEND [SERIES]: Action

[Diagram showing Fortinet-VPN logon details]

- Action: negotiate
- IP Addresses: 62.34.123.14, 123.230.14.00, 1270.0.1, 123.231.60.204

10/29 17:21 - 10/30 17:21